

Application Serial No. 09/980,271 - Filed November 30, 2001

REMARKS

Claims 1-11 are pending.

In the present Office Action, claims 1-11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,338,138 (hereinafter "Raduchel"), in view of U.S. Patent No. 6,122,741 (hereinafter "Patterson"). Applicant submits each of the pending claims recite features neither taught nor suggested by the cited art, either singly or in combination. Accordingly, Applicant traverses the above rejections and requests reconsideration.

Pending claim 1 recites a system for authenticating a PIN code of a user in an interactive information system in order to run an application, the system comprising:

"an input device for entering a PIN code of a user;

a security manager configured to:

receive a request for user authentication from the application;

compare a received PIN code of the user with a registered PIN code, in response to said request;

supply information to the application about PIN code entering key-pressing operations by the user, wherein the entered PIN code is not supplied to the application; and

give authorization to run said application if the PIN code of the user matches the registered PIN code;

wherein the application is configured to present a PIN entry field, wherein crypted information corresponding to said information about PIN code entering key-pressing operations received from the security manager is displayed in the PIN entry field."

It is first noted that the presently claimed invention and the cited art are generally directed to different ends. The presently claimed invention is generally directed to a

Application Serial No. 09/980,271 - Filed November 30, 2001

system and method for authenticating a user's PIN in order to run an application. In contrast, Raduchel is directed to a network based logon procedure whereby a user may logon to a local computer.

In the above recitation there is a direct relationship between a particular application and authorization to run the particular application. It is noted that the recited request for user authentication is supplied "from the application." The authorization signal is then given "to said application" to "run said application." In contrast, Raduchel discloses a browser/applet receives a user's login information and conveys that login information to a remote authentication manager. For example, Raduchel discloses:

"Methods and systems consistent with the present invention are described in greater detail with reference to FIG. 2, which depicts a flowchart of the steps performed at start-up time of local computer 101. When the local computer is initially started, a small portion of the operating system is loaded (step 202). In this step, the minimum code necessary to run authentication is loaded, including VM 117 as well as the minimum components of the operating system necessary to load and run a web browser; it does not include a command interpreter or file capabilities. Next, the browser is loaded and run (step 204). As shown in FIG. 3, when running the browser, the user is initially presented with a screen 300 having a login dialog box 302 into which the user can enter their username and password. This screen is displayed by an applet, stored with the browser, that performs authentication by communicating with the authentication manager. In an alternative embodiment, the user enters a user name and is prompted with a challenge number which is entered into a digital token card and the resulting password is entered into the system. In another alternative embodiment, the local computer includes a smartcard reader and the user inserts a smartcard into the reader. However received, the authentication information, including the username and password, is sent by the browser to the authentication manager using the well-known HyperText Transfer Protocol (HTTPS), and using the well-known Secure Socket Layer (step 206)." (Raduchel, col. 4, line 58 – col. 5, line 16).

In addition to the above, Raduchel discloses:

Application Serial No. 09/980,271 - Filed November 30, 2001

"Returning to FIG. 2, the local computer receives the authentication results from the authentication manager and determines if the user was authenticated (step 208). If authentication fails . . . the user is allowed only to perform actions considered non-invasive, such as sending and receiving e-mail, viewing publicly available, non-proprietary web pages via the browser, or viewing on-line calendars. However, if authentication is successful, the user may use all of the available services of the local computer. . . .

If authentication fails, the browser provides the user with restricted access to the local computer (step 210). In this step, the browser displays icons representative of the services that the user may use, as indicated in the token received from the authentication manager. For example, FIG. 5 depicts the browser screen 300 with three icons: icon 502, allowing the user to access an e-mail system; icon 504, allowing the user to use a time management program; and icon 506, allowing the user to browse various web pages on the Internet. Upon selecting one of the icons 502-506 for the first time, the browser sends a request to the authentication manager for the appropriate service applet, and the authentication manager downloads it to the browser so that the user may use the corresponding service. Subsequent selections of the icon do not cause a download of the service applet; instead, recognizing that a copy has already been downloaded, the browser merely invokes that copy." (Raduchel, col. 5, lines 32-62). (emphasis added).

From the above, it can be seen that Raduchel discloses the browser receives and sends the authentication information to the authentication manager. The authentication manager then returns a token to the local computer which indicates success or failure. If a failure is indicated, some subset of services of the local computer may be indicated by the token as authorized/usable by the user. Accordingly, there is no direct relationship between an application and authorization to run the application as recited. As noted above, the claims recites a direct relationship between a particular application and authorization to run the particular application. Further, the request for user authentication is supplied "from the application" (i.e., the application the user desire to run). Finally, the authorization signal is then given "to said application" to "run said application." These features are not disclosed by the cited art, either singly or in combination. For at least these reasons, each of the independent claims are patentably distinguishable from the cited art and a prima facie case of obviousness has not been established.

Application Serial No. 09/980,271 - Filed November 30, 2001

In addition to the above, the cited art does not disclose a security manager configured to "supply information to the application about PIN code entering key-pressing operations by the user, wherein the entered PIN code is not supplied to the application." First, as discussed above, Raduchel does not disclose the security manager supplying the information to "said" application as recited. Second, Raduchel includes no teaching or suggestion of a security manager supplying information concerning PIN code key-pressing operations to the application without the PIN code being supplied to the application. These features are nowhere found in the cited art. Column 5, lines 17-35 are cited as disclosing these features. However, this disclosure of Raduchel merely states:

"The authentication manager receives the log-in information and uses it to authenticate the user, as shown in FIG. 4. Although various embodiments of the authentication manager may vary and could be configurable, in one implementation, the authentication manager receives a log-in request containing a user name and password (step 402 in FIG. 4). After receiving this information, the authentication manager authenticates the user by accessing the authentication file to determine if the user name and password are contained in it (step 404) and returns a token that identifies the services that the user may use (step 406). Additionally, this token may contain a profile of the user's access rights, and when the token is returned to the local computer, it would be included in all further requests from the local computer. Returning to FIG. 2, the local computer receives the authentication results from the authentication manager and determines if the user was authenticated (step 208)." (Raduchel, col. 5, lines 17-34).

Clearly, the above disclosure does not describe a security manager supplying information concerning key-pressing operations to the application. Rather, the remote authentication manager receives the complete authentication information from the local computer, performs an authentication check, and returns a result to the local computer. Further, there is no disclosure of providing such key-pressing information without providing the PIN code. Therefore, for at least these additional reasons, each of the independent claims are patentably distinct from the cited art.

Application Serial No. 09/980,271 - Filed November 30, 2001

Still further, claim 1 recites the additional features wherein "the application is configured to present a PIN entry field." In other words, the application for which the user seeks authorization to run presents the PIN entry field. As already discussed above, the cited art does not disclose the application in the manner recited. Accordingly, these features are not disclosed by the cited art.

Finally, as each of the dependent claims includes the features of the independent claims upon which they depend, the dependent claim are patentable for at least the reasons given above.

In addition to the above, Applicant notes that neither claim 5 nor claim 6 are addressed in the present office action.

Applicant believes the application to be in condition for allowance. However, should the examiner believe issues remain which would prevent the present application from proceeding to allowance, the below signed representative requests a telephone interview to facilitate a more speedy resolution.

Application Serial No. 09/980,271 - Filed November 30, 2001

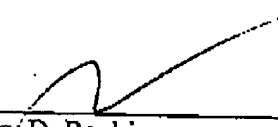
CONCLUSION

Applicant submits the application is in condition for allowance, and an early notice to that effect is requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5266-09100/RDR.

☒ A Return Post Card

Respectfully submitted,



Rory D. Rankin
Reg. No. 47,884
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin,
Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8800

Date: June 20, 2006